**П Р А В И Л Н И К**

**О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНОГ СИСТЕМА**

**АДВОКАТСКЕ КОМОРЕ ЧАЧАК**

ЧАЧАК, август 2020.

Управни одбор Адвокатске коморе Чачак, на основу члана 66 Закона о адвокатури („Службени гласник РС“ 31/2011, 24/2012 – ОУС), члана 9., члана 30. став 1 тачка 35, члана 260. Статута Адвокатске коморе Чачак („Службени лист Града Чачка“ 9/2012), члана 8 Закона о информационој безбедности (Службени гласник РС 6/16), члана 2 и 3 Уредбе о ближем уређењу мера заштите информационо – комуникационих система од посебног значаја („Службени гласник РС“ 94/2016), донео је:

**П Р А В И Л Н И К**

**О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНИХ СИСТЕМА**

**АДВОКАТСКЕ КОМОРЕ СРБИЈЕ**

1. **УВОДНЕ ОДРЕДБЕ**

**Члан 1.**

Правилником о безбедности информационо – комуникационих система Адвокатске коморе Чачак (у даљем тексту: Правилник) се ближе дефинишу и утврђују мере заштите информационо – комуникационих система (у даљем тексту: ИКТ систем), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса Адвокатске коморе Чачак (у даљем тексту: Комора).

**Члан 2.**

Циљеви доношења Правилника су:

1. Прописивање процедура коришћења и заштите информационо – комуникационих система Коморе;
2. Прописивање овлашћења и одговорности запослених у вези са приступањем, коришћењем и у вези са безбедношћу и ресурсима ИКТ система;
3. Минимизација безбедносних ризика на начин да се спречи настанак и ублаже последице инцидената којима се угрожава или нарушава информациона безбедност;
4. Подизање нивоа опште свести, а посебно запослених у Стручној служби Коморе (у даљем тексту: Служба) о ризицима и опасностима које су везане за коришћење информационих технологија;
5. Унапређење и развој одговарајућих безбедносних апликација и обезбеђивање сталне контроле свих компоненти информационо – комуникационих система;
6. Складиштење и чување података на начин који обезбеђује приступ истима само од стране овлашћених лица;
7. Свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

**Члан 3.**

Мере заштите ИКТ система, овлашћења и одговорности запослених у вези са приступањем, коришћењем и безбедности података и ресурса ИКТ система служе превенцији од настанка инцидената и минимизацији штете од евентуалних инцидената и њихова примена је обавезна за све запослене.

Запослени у Служби Коморе морају бити упознати са садржином овог Правилника и дужни су да поступају у складу са Законом о заштити података о личности и овим Правилником, као и са процедурама које регулишу приступање, коришћење, безбедност и ресурсе ИКТ система.

**Члан 4.**

Запослени у Служби Коморе су дужни да приступају инфромацијама и ресурсима ИКТ система само ради обављања редовних радних задатака и да редовно и благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби овог Правилника, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

**Члан 5.**

Мере заштите ИКТ система се односе на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управqа ИКТ системом, корисничке налоге, тајне информације за ру веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

**Члан 6.**

Адвокатска комора Чачак врши јавна овлашћења у складу са одредбом члана 65 Закона о адвокатури и ради обављања послова из своје надлежности прикупља, обрађује, користи за потребе одлучивања у управном поступку о статусним питањима адвоката и адвокатских ортачких друштава и чува податке који су заштићени Законом о заштити података о личности.

**Члан 7.**

Поједини термини који се користе у функционисању ИКТ система имају следеће значење:

1. Информационо – телекомуникациони систем (ИКТ систем) је технолошко организациона целина која обухвата:
2. Електроноске комуникационе мреже у смислу закона који уређује електронске комуникације,

б) Уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма,

в) Податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке а) и б) ове тачке у сврху њиховог рада, употребе, заштите и одржавања,

г) организациону структуру путем које се управља ИКТ системом;

1. Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност, и непорецивост тих података да би тај систем функционисао како је предвиђено под контролом овлашћених лица;
2. Тајност је својство које значи да податак није доступан неовлашћеним лицима;
3. Интегритет значи очуваност изворног садржаја и комплетност података;
4. Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
5. Аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онак за које је декларисано да је ту радњу извршио;
6. Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
7. Ризик значи могућност наруштавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
8. Управљање ризиком је систематичан скуп мера који укључује планирање,м организовање и усмеравање активности коко би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
9. Инцидент је унутрашња или спољна околности или догађај којим се угрожава или нарушава информациона безбедност;
10. Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
11. Тајни податак је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеним у складу са законом, одређен и означен одређеним степеном тајности;
12. ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
13. Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде, или чувања података чијим пријемом и анализом се може открити садржај тих података;
14. Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
15. Криптозаштита је примена метода, мера и поступака ради трансформисања података у облика који их за одређено време или трајно чини недоступним неовлашћеним лицима;
16. Криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
17. Криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
18. Безбедносна зона је простор у коме се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
19. Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње правилнике, процедуре и слично;
20. Бекап је резервна копија података;
21. Архивирање података је процес складиштења посебно одабраних података за дугорочно чување и њихово будуће референцирање;
22. VPN (*Vitrual Private Network*) је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојемим локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
23. MAC адреса (*Media Access Control Address*) јесте јединствени број, којим се врши идентификација уређаја на мрежи;
24. Download је пренос података са централног рачунара или веб презентације на локални рачунар;
25. UPS (*Uninterruptible powe supply*) је уређај за непрекидно напајање електричном енергијом;
26. Freeware је бесплатан софтвер;
27. Open – source је софтвер отвореног кода;
28. Firewall је „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информације између локалне мреже и интернета ради онемогућавања злонамерних активности;
29. USB, CD-ROM, DVD, флеш меморија, екстерни хард – дискови, касете јесу спољашњи медијуми за складиштење података.
30. **МЕРЕ ЗАШТИТЕ**

**Члан 8.**

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидентата, односно превенција и минимизација штете од инцидентата који угрожавају вршење надлежности и обављање делатности Коморе, а посебно у оквиру пружања услуга члановима Коморе, али и другим лицима у вези са радом Коморе или размене података са другим државним органима у циљу остваривања права чланова Коморе.

Описи мера су груписани у 28 одељака, према називима и редоследу тачака који су утврђени Законом о информационој безбедности.

1. **Успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Коморе**

**Члан 9.**

Сваки запослени у Служби, као корисник ИКТ система Коморе, одговоран је за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности. Комора у оквиру организационе структуре утврђује послове и одговорности корисника ИКТ система ради управљања информационом безбедношћу.

Обавезе и одговорности запослених у Служби као корисника ИКТ система прописани:

* Правилником о систематизацији радних места Адвокатске коморе Чачак,
* Правилником о именицима, евиденцијама и заштити података о личности Адвокатске коморе Србије,
* Правилником о налозима и страницама на друштвеним мрежама Адвокатске коморе Србије
* Правилником о канцеларијском и архивском пословању у адвокатским коморама, адвокатским канцеларијама, заједничким адвокатским канцеларијама и адвокатским ортачким друштвима Адвокатске коморе Србије
* Уговорима о раду
* Изјавом о поверљивости.

**Члан 10.**

Под пословима из области безбедности ИКТ система утврђују се:

* Послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност,
* Послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности,
* Послови инемогућавања, односно спречавања неовлашћене или ненамерне измене оштећења или злоупотребе средстава, односно информационих добара ИКТ система Коморе, као и приступ, измена или коришћења средстава без овлашћења и без евиденције о томе,
* Праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
* Обавештавање надлежних органа о инцидентима у ОКТ систему, у складу са прописима.

1. **Постизање безбедности рада на даљину и употреба мобилних уређаја**

**Члан 11.**

Комора дозвољава рад на даљину под одређеним условима и специфичним ситуацијама када због постојања посебних услова није могућ рад у пословним просторијама Коморе.

Под радом на даљину подразумева се: рад ван пословних просторија, рад д куће и виртуално радно окружење, а односи се на ситуацију када је запослени обавезан да изврши одређене послове на мрежи послодавца, а налази се ван пословних просторија Коморе.

Рад на даљину је дозвољен под условом да запослени који ради на даљину приступ бази података на централном рачунару (серверу) приступа преко регистрованог преносног рачунара (лаптопа) – мобилног уређаја који је у власништву Адвокатске коморе Србије и које запослени преузме уз потписивање реверса о коришћењу ван пословних просторија Коморе уз навођење адресе коришћења уређаја и временског периода у коме се одвија рад на даљину. У случају губитка или крађе преносног уређаја, корисник је дужан да одмах обавести руководиоца Службе и председника Коморе и пријави крађу/губитак надлежном јавном тужилаштву, односно Министарству унутрашњих послова. Лице које одржава ИКТ систем Коморе, дужно је да одмах по пријему налога руководиоца Службе, укине дозволу приступа централном рачунару за регистровани преносни (мобилни) уређај.

Рад на даљину је дозвољен под условом да запослени који ради на даљину приступ бази података на централном рачунару (серверу) приступа преко сопственог рачунара који у том случају мора бити регистрован у бази података о овлашћеним корисницима преко MAC и IP адресе.

Уређаји морају бити тако подешени да омогуће сигуран и безбедан приступ ИКТ систему коришћењем VPN и уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Захтев за приступ локалној мрежи Коморе који морају бити испуњени и дефинисани у VPN процедури су:

* Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама,
* Ауторизовани корисници морају чувати креденцијалне својих налога и не смеју омогућити приступ било ком трећем лицу,
* Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи Коморе, ауторизовани корисник не сме истовремено бити повезан и на другу мрежу која може угрозити безбедност комуникације,
* Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења VPN процедуре,
* сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима.

Приступ ресурсима ИКТ система се региструје, надзире и чува у бази података одговарајућег програмског решења који одобрава и контролише приступ централном рачунару.

Кориснички уређаји са којих ће се приступати ресурсима ИКТ система, могу се користити у оквиру заштићене интернет везе за обављање послова из надлежности Коморе и у периоду када није могућ рад у просторијама Коморе.

Запосленима (аутеризованим корисницима) није дозвољено да коришћење локалне мреже Коморе за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада.

Рад на даљину запослених одобрава Управни одбор и председник Коморе.

**Члан 12.**

Мобилни телефони, пресонални рачунари, таблет уређаји лица која нису запослена у Служби не могу се регистровати на заштићеној интернет вези која се користи за обављање послова из надлежности Коморе.

Приликом боравка у просторијама Коморе, трећим лицима (члановима органа Коморе, посетиоцима и сл.) може се омогућити приступ одвојеној интернет вези која није повезана са радом централног компјутера и преко које се не врши пренос службених података са централног компјутера ка локалним радним јединицама и у обрнутом смеру.

**Члан 13.**

Омогућавање обављања задатих и неопходних послова на даљину, уређује се путем процедуре за VPN приступ информационом систему Коморе.

Правилном применом утврђеног поступка и начина приступа, Комора своди на минимум потенцијалну изложеност штети која може настати услед неовлашћеног или неконтролисаног пристума локалној мрежи Коморе.

Сви пословни подаци који се креирају приликом рада на даљину, складиште се на централном компјутеру и у информационом систему Коморе.

**Члан 14.**

Корисницима ИКТ система забрањена је самостална инсталација софтвера и подешавање службених уређаја, као и давање тих уређаја другим неовлашћеним лицима.

Лица која одржавају ИКТ систем Коморе, приликом инсталације програма и уређаја, морају да користе искључиво лиценциране програме и атестиране уређаја.

1. **Обезбеђивање да лица која користе ИКТ систем, односно управљају ИКТ системом буду оспособљена за посао који обављају и разумеју своју одговорност**

**Члан 15.**

Управљање ИКТ системом подразумева одржавање у исправном стању VPN мреже и свих уређаја који су регистровани као корисници те мреже, а посебно да VPN мрежа и уређаји буду заштићени адекватном Firewall „заштитним зидом“ односно системом преко кога се врши надзор и контролише проток информације између локалне мреже и интернета ради онемогућавања злонамерних активности.

Послове одржавања у исправном стању VPN мреже, свих компјутерских уређаја који су регистровани корисници ИКТ система Коморе, инсталацију лиценцираних програма и атестираних уређаја Комора може поверити специјализованом привредном друштву или предузетнику које/који располаже потребним знањима, стручно је оспособљено и поседује потребне лиценце за правилан и стручан рад и са њим закључити посебан уговор којим ће бити регулисана права, дужности и одговорности уз обавезу потписивања изјаве о поверљивости.

Послове израде, дораде, одржавања софтверског решења програма Именик адвоката који се користи у свакодневном раду Комора може поверити специјализованом привредном друштву или предузетнику или аутору програма које/који располаже потребним знањима, стручно је оспособљено и поседује потребне лиценце за правилан и стручан рад и са њим закључити посебан уговор којим ће бити регулисана права, дужности и одговорности уз обавезу потписивања изјаве о поверљивости у којима ће бити јасно наведено да је Комора власник програма и поштовање ауторских права.

Свако коришћење ИКТ ресурса Коморе од стране корисника ИКТ система мимо прописаних правила и процедура, као и додељених овлашћења подлеже дисциплинској, прекршајној или кривичној одговорности.

1. **Заштита од ризика који настају при променама послова или престанка радног односа запосленог у Служби Коморе**

**Члан 16.**

Сви запослени, као корисници ИКТ система су дужни да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система Коморе и након престанка или промене радног ангажовања.

Промене врсте и обима овлашћења за приступ ИКТ систему Коморе ће се извршити у складу са описом послова на које запослени буде распоређен, односно укинут уколико му престане радни однос у Служби Коморе, на основу захтева руководиоца Службе и председника Коморе.

1. **Идентификовање информационих добара и одређивање одговорности за њихову заштиту**

**Члан 17.**

Информациона добра Коморе су сви ресурси који садрже пословне информације и информације које су заштићене Законом о заштити података о личности, а односе се на личне податке адвоката и адвокатских приправника који су уписани или су били уписани у Именик адвоката, односно у Именик адвокатских приправника Коморе, односно путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарскоу опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компоненти, техничку и корисничку документацију и правилнике и упутства који се односе на ИКТ систем и сл.

Предмет заштите су:

* Хардверске и софтверске компоненте ИКТ система,
* Апликације и сервиси Коморе,
* Подаци који се чувају или обрађују на компонентама ИКТ система Коморе,
* Кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система;
* Комуникациони линкови.

**Члан 18.**

Комора врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. Комора прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином најмање једном годишње.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води Комора преко овлашћеног радника Службе, преко лица са којим има закључен уговор о креирању и одржавању ИКТ система и преко лица са којима има закључен уговор о изради програмских апликација за програме Именик адвоката.

**Члан 19.**

Запослени којима је дато на коришћење имовине која се односи на информациона добра и ИКТ систем су дужни да правилно управљају повереном имовином током целог животног циклуса.

Запослени су обавезно да врате сву имовину која је у власништу Коморе коју користе након престанка уговора о раду. Ову обавезу имају и лица која су ангажована по основу уговора за израду и одржавање ИКТ система и израду програмских апликација Именик адвоката и Кол центра који су дужни да предају програмске кȏдове и кључеве (почетну апликацију и све измене и дораде апликације) које су извршене до раскида уговора и све копије програма које су евентуално сачињене.

**Члан 20.**

Управни одбор и Председник Коморе дужни су да захтевају од свих запослених да примењују мере заштите безбедности у складу са овим Правилником и важећим процедурама.

Комора у циљу развоја, имплементације и одржавање система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

* Обезбеђује да се поступци заштит спроводе на организован начин и у складу са процедурама и у континуитету,
* Штити информације и податке са дефинисаним профилом осетљивости и карактеристикама на једнак начин,
* Спроводи програм заштите на конзистентан и уједначен начин,
* Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

**Члан 21.**

Запослени у Служби Коморе су обавезни да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација на начин који одговара радном месту на које су распоређени.

1. **Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности**

**Члан 22.**

Подаци који се налазе у ИКТ систему представљају пословну тајну ако су тако дефинисани одредбама посебних прописа: Закона о слободном приступу информацијама од јавног значаја, Закона о заштити података о личности, Закон о тајности, Уредбе о начину и поступку означавања тајности података, односно докумената и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо – телекомуникационим системима.

**Члан 23.**

Класификациона шема поверљивости информација се базира на четири нивоа:

* Откривање не изазива никакву штету,
* Откривање изазива мању непријатност или мању штету,
* Откривање има значајан краткорочни утицај на пословање или тактичке циљева,
* Откривање иа озбиљан утицај на дугорочне стртешке циљеве.

Класификација се врши ради:

* Јачање корисничке одговорности како би запослени могли да уоче и препознају вредност података приликом пру+икупљања, обраде, чувања или слања и постану свесни за неовлашћено коришћење или преношење,
* Подизање свести о вредности информације или документа,
* Заштите података у покрету ради боље и интелигентије интеграције и осталим производима за заштиту параметара и крајњих уређаја,
* Заштите садржаја,
* Интеграције са системима за архивирање.

Процедура о поступању са имовином мора да подразумева:

* Ограничење приступа која подржавају захтеве за заштиту сваког нивоа класификације,
* Одржавање званичног записа о овлашженим примаоцима имовине,
* Заштиту привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације
* Складиштење информационе имовине у складу са спецификацијама произвођача,
* Јасно обележавање свих копија медија на које овлашћени прималац треба да обрати пажњу.

1. **Заштита носача података**

**Члан 24.**

Комора обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података коју се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци води руководилац Службе.

Заштита података и њихових носача обезбеђује се процедурама које се поштују током рада које доприносе:

* Да се подаци и документи (посебно они са ознаком тајности) снимају на сервере, у фолдере над којима право приступа има само запослени коме је одобрен приступ,
* Да се подаци и документи (посебно они са ознаком тајности) снимају и на друге носаче (екстерни хард диск, USB, CD, DVD) над којима ће право приступа имати само корисници ИКТ система којима је то право одобрено.

**Члан 25.**

Подаци о преносним носачима садрже следеће одредбе:

* Садржај сваког медијума који се може поновно користити и који ће се износити изван пословних просторија, а када више није потребан треба да се неповратно избрише,
* Податке о медијима који се могу износити из пословних просторија када је то неопходно и изводљиво и за које је потребно захтевати одобрење, а о свим таквим изношењима треба водити евиденцију како би се сачувао траг за проверу,
* Све медијуме треба складиштити на безбедном и заштићеном месту,
* Коришћење криптографских техника за заштиту података на преносним медијумима, ако су поверљивост или интегритет података важни,
* Подаци треба да буду пренети на нови медијум пре него што постану нечитљиви,
* Вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података,
* Мачин регистровања преносних медија у циљу ограничавања могућности губљења података,
* Покретне преносне медијуме треба користити само ако за то постоји пословна потреба,
* Уколико постоји потреба за коришћењем прносних медијума, неопходно је пратити пренос података на те медијуме.

**Члан 26.**

Када више нису потребни, медијуми се расходују на безедан начин како би се свео на минимум ризик од могућег преузимања осетљивих података од стране неовлашћених особа.

Медијуме који садрже остељиве податке треба расходовати спаљивањем или идањем или брисање података ради коришћења у неком другом апликативном програму унутар Коморе.

Расходовање медијума који садрже осетљиве податке је потребно евидентирати како би се сачувао траг за проверу.

**Члан 27.**

Носачи података који садрже информације које се штите од неовлашћеног приступа, злопотребе или оштећења приликом транспорта, уколико поверљива информација на медијуму није шифрована, мора бити додатно физички заштићен.

Уколико се тај медијум мора транспортовати ван пословног простора Коморе, мора се обезбедити безбедан транспорт и користити поуздан транспорт или курира, увести проверу курира, а опрема за пренос мора бити таквог карактера да обезбеди заштиту од свих физичких оштећења која би могла настати током преноса.

1. **Ограничење приступа подацима и средствима за обраду података**

**Члан 28.**

Приступ ресурсима ИКТ система је одређен врстом налога, односно додељеним овлаштењима које користини ИКТ система имају.

Лица која имају администраторски налог имају право приступа ресурсима ИКТ система (софтверским, хардверским, мрежним, мрежним ресурсима, програмским апликацијама) ради инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

**Члан 29.**

Корисници ИКТ система могу да користе само свој кориснички налог који су добили од администратора система и не смеју да омогуће другом лицу коришћење његовог корисничког налога, сем администратору система за подешавање корисничког прогила и радне станице.

Корисници ИКТ система дужни су да поштују следећа правила безбедног и примереног коришћења ресурса ИКТ система и то:

1. Да користе информатичке ресурсе искључиво и у пословне сврхе,
2. Да прихвате да су сви подаци који се прикупљају, обрађују, складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Коморе, а лични подаци из Именика адвоката и Именика адвокатских приправника који су заштићени Законом о заштити података о личности су власништво Коморе и лица на које се ти подаци односе,
3. Да поступа са поверљивим посацима у складу са прописима, посебно приликом копирања или преноса података,
4. Да безбедно чувају своје лозинке, односно да их не преносе другим лицима,
5. Да мењају лозинке сагласно утврђеним правилима,
6. Да поднесу захтев за инсталацију софтвера или хардвера у писаној форми, одобран од стране непосредног руководиоца,
7. Да приступају информатичким ресурсима само на основу додељених корисничких права,
8. Да обезбеде сигурност података у складу са важећим прописима,
9. Да не заустављају рад и не бришу антивирусни програм, не мењају његове подешене опције, не инсталирају неовлашћено други антивирусни порграм,
10. Да не складишти садржај на радној станици, н и ти садржај оји не служи у пословне сврхе,
11. Да израђују заштитне копије (бекап) података у складу са прописаним процедурама,
12. Да користе интернет и електронску пошту у складу са прописаним процедурама,
13. Да прихвате да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл) обављају у одређено време,
14. Да прихвате да сви приступи информатичким ресурсима и информацијама буду засновани на принципу минималне неопходности,
15. Да прихвате технике сигурности (антивирусни програми, заштитни зидови, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему,
16. Да не инсталирају, не модификују, не искључују из рада или бришу заштитни, системски или апликативни софтвер.
17. **Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа**

**Члан 30.**

Право приступа ИКТ система Коморе имају сви корисници који приступају заштићеним ресурсима из пословних разлога и имају само један доменски налог којим приступају свим ресурсима коју се неопходни за обављање пословних задатака.

Налог се користи од корисничког имена и лозинке, на основу којих се врши аутентификација (провера идентитета) и ауторизација (провера права приступа).

Налози могу бити администраторски и кориснички.

Администраторски налог је налог преко кога администратор система води евиденцију о корисничким налозима, на основу захтева запосленог који је одобрен од стране руководиоца Службе.

Кориснички налог је налог који додељује администратор система, након уноса података о запосленом у систем у складу са потребама обављања радних задатака.

Сваком запосленом се одобрава – додељује приступ и обим овлашћења у складу са радним задацима које обавља. Одобравањем приступа се додељују јединствени подаци за логовање који се не могу делити са другим корисницима.

Привилегована права на приступ која треба доделити неком кориснику ИКТ система су другачија од оних која се користе за редоне активности. Овлашћења корисника са привилегованим приступима се редовно испитују ради провере да ли су у складу са његовим радним обавезама и одговорностима.

Запосленом коме престане радни однос у Служби АКС укида се право на приступ ИКТ систему.

1. **Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију**

**Члан 31.**

Аутентификација корисника којима је одобрен приступ се врши путем корисничког имена и лозинке.

Сви корисници су дужни да привремене шифре промене приликом првог пријављивања, да корисничко име и лозинку држе у тајности и не откривају другим лицима, укључујући и надређене особе, да избегавају чување корисничког имена и лозинке у писаном облику и да промене лозинку увек када постоји било какав наговештај могућег компромитовања. Шифре морају да садрже најмање 9 алфанумеричких карактера, најмање једно велико и 1 мало слово и најмање један број од 0 – 9.

1. **Предвиђање одговарајуће криптозаштите ради заштите тајности, аутентичности односно интегритета података**

**Члан 32.**

У Комори није предвиђена криптозаштита.

Ради заштите тајности, аутентичности и интегритета података, Комора може да уведе одговарајуће мере криптозаштите за податке које се налазе у Именику адвоката, Именику адвокатских приправника и Кол центру.

1. **Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему**

**Члан 33.**

Комора је дужна да предузме мере ради спречавања неовлашћеног приступа објекту, простору и просторијама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Просторије у којима се налази опрема за обраду информација морају бити физички обезбеђене на одговарајући начин што подразумева: стални надзор запослених у радно време, закључана и обезбеђена врата са додатним заштитним механизмима: контролном камером и алармима.

У просторије Коморе могу ући само лица која имају пословни разлог за боравак у пословним просторијама. Улазак у пословне просторије у радно време контролишу запослени, а ван радног времена у пословним просторијама Коморе није дозвољен боравак лица који нису запослена у Служби Коморе. Под радним временом подразумева се радно време од понедељка до петка у времену од 08 до 15 часова, а викендом и после 15 часова само у случају одржавања састанака органа Коморе.

**Члан 34.**

С обзиром на врсту и број опреме коју користи Комора за обављање послова из своје надлежности није потребно формирање посебне сервер собе да посебним мерама заштите.

1. **Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем**

**Члан 35.**

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

Улаз у простор у коме се налази део ИКТ опреме дозвољен је само оператерима ИКТ система, запосленима у Служби Коморе који обављају послове од значај за обраду информација на ИКТ систему.

Приступ ИКТ систему могу имати и трећа лица ради инсталације и сервисирања одређених ресурса ИКТ система уз присуство запосленог у Служби Коморе, као и лица који раде на пословима хигијенско – техничког одржавања простора и инсталација.

1. **Обезбеђивање исправног и безбедног функционисања средстава за обраду података**

**Члан 36.**

Коришћење ресурса ИКТ система се надгледа, подешава и пројектује у складу са потребама и захтеваним капацитетима у наредном периоду, како би се осигурале захтеване карактеристике система.

Запослени у Служби Коморе и лица која су ангажована по уговору на пословима ИКТ система стално надзиру и проверавају функционисање средстава за обраду и чување података и управљају ризицима који могу утицати на безбедност ИКТ система и у складу са тим предлажу одговарајуће мере.

**Члан 37.**

Пре увођења у продукцију новог софтвера, неопходно је направити копију – архиву постојећих података ради припрема за процедуту враћања на претходну стабилну верзију. Инсталирање новог софтвера, као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад корисника ИКТ система. У случају да се у новој верзији софтвера који је уведен у оперативни рад примете битни недостатци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

За развој и тестирање софтверам пре увођења у ОКТ систем, морају се користити уређаји и подаци који су намењени тестирању и развоју апликативних решења. При тестирању се мора обезбедити несметано функционисање ИКТ система. Забрањено је коришћење сервера који се користе за оперативни рад за тестирање софтвера на начин који може да заустави нормално функционисање ИКТ система.

**Члан 38.**

У циљу обезбеђивања непрекидности рада ИКТ система потребно је обезбедити опрему која штити од прекида напајања тако што се:

* Помоћна опрема за напајање набавља у складу са процењеним потребама за непрекидан рад ИКТ система,
* Помоћна опрема одржава у складу са спецификацијама произвођача опреме и прописима,
* Капацитет помоћне опреме редовно процењује,
* Помоћна опрема се редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова,
* Обезбеђује вишеструко напајање, у случају потребе, са различитих траса.

**Члан 39.**

Каблови за напајаре и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама се штите од прислушкивања, оматања или оштећења на начин који обезбеђује највиши ниво заштите у складу са техничким и грађевинским могучностима у згради у којој се налазе пословне просторије Коморе.

**Члан 40.**

Опрема се одржава редовно како би се осигурала њена непрекидна расположивост и неповредивост на следећи начин:

* Одржавање у складу са препорученим сервисним интрвалима у према спецификацији произвођача опреме,
* Поправке и сервисирање опреме може да обавља само лице које је оспособљено за одржавање ове врсте опреме на основу уговора са Комором,
* О свим сумњивим или стварним неисправностима, као и о целокупном превентивном или корективном одржавању чувају се записи,
* Осетљиве информације треба избрисати из опреме, уколико је потребно поједине елементе ИКТ система изнети ван пословних просторија Коморе ради поправке;
* Пре враћања у рад опрема након одржавања потребно је исту прегледати и проверити да ли је неовлашћено коришћења или оштећења или на њој инсталирани програми који могу угрозити безбедност и рад ИКТ система Коморе.

**Члан 41.**

Опрема, информације или софтвер који се користи за рад ИКТ система могу да се измештају из пословних просторија Коморе само уз одобрење одговорног лица тако што ће се документовати идентитет и улога лица који користе и поступају са опремом приликом премештања и ова документација треба да буде враћена са опремом и информацијама или софтвером по престанку разлога због који су ресурси ИКТ система Коморе били премештани и то тако што ће се сачинити записник у коме се наводи назив и тип опреме, серијски број, назив овлашћеног сервиса и име и презиме овлашћеног лица сервиса који је преузео опрему из просторија Коморе. Уговором са овлашћеним сервисом морају бити дефинисане обавезе у погледу заштите података који се налазе на медијима коју су део ИКТ ресурса Коморе.

На измештену опрему треба применити безбедносне механизме заштите.

Сви делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњенили или реинсталирани.

**Члан 42.**

Запослени у Служби треба да обезбеде да опрема која је без надзора и ван радног времена има одговарајућу заштиту како би се онемогућио приступ заштићеним информацијама и подацима.

Сва осетљива и поверљива документа, материјали и информације морају бити склоњени са радне површине и одложени на одговарајуће место које се закључава када запослени није на свом радном месту или када се документа, материјали и информације не користе.

1. **Заштита података и средстава за обраду података од злонамерног софтвера**

**Члан 43.**

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете ресурсе ИКТ система Коморе.

Заштита података и средстава за обраду података од злонамерног софтвера се заснива на превенцији и откривању злонамерног софтвера, отклањању штете, одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

Заштита од злонамерног софтвера на мрежи се спроводи ради заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.).

Комора одређује и примењује контроле откривања, спречавања и опорвака ИКТ система ради заштите од злонамерног софтвера. За успешну заштиту од вируса инсталира се антивирусни програм (на серверу и радним станицама) и свакодневно се аутоматски врши допуна антивирусних дефиниција.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија. Преносиви медији, пре коришћења, морају бити проверени на присуство вируса, а ако се утврди да садрже вирусе, уколико је то могуће, врши се чишћење медија антивирусним софвером. Уколико чишћење од вируса преносивог медија није могуће, тај медиј се одмах уклања из ресурса ИКЗ система Коморе и уништава на безбедан начин. Ризик од евентуалног губитка података приликом чишћења медија од вируса преузима доносилац медија.

Ради сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

* Електронска пошта са прилозима се не сме отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати,
* Забрањено је коришћење електронске поште у приватне сврхе,
* Не смеју се користити приватни налози електронске поште и пословне сврхе.

У случају да корисник примети необично понашање рачунара, запажање треба да, без одлагања, пријави лицу са којим Комора има закључен уговор о одржавању опреме.

1. **Заштита од губитка података**

**Члан 44.**

Заштита од губитка података у Комори се врши израдом резервних копија које обухватају системске информације, апликације и податке који су неоходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Прављење заштитних копија и заштита од губитка података обавља се на дневном нивоу, праве се најмање две резервне копије свих података ИКТ система Коморе, као и копија на екстерном медијуму. Једна заштитна копија се налази у просторијама Коморе, друга на удаљеном унапред дефинисаном месту и копија на екстерном медијуму код руководиоца Службе Коморе.

1. **Чување података о догађајима који могу бити од значаја за безбедност ИКТ система**

**Члан 45.**

У ИКТ систему Коморе формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу информација који се морају чувати и редовно преиспитивати.

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

1. **Обезбеђивање интегритета софтвера и оеративних система**

**Члан 46.**

У ИКТ систему Коморе може да се инсталира смо лиценцирани софтвер и софтвер који је одобрен од стране Коморе која спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.

Инсталацију и подешавање софтвера може да изврши само лице које има овлашћење за то у складу са уговором о набавци односно одржавању софтвера.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

1. **Заштита од злоупотреба техничких безбедносних слабости ИКТ система**

**Члан 47.**

Комора периодично, а најмање једном годишње, врши анализу ИКТ система и утврђује степен ризика изложености ИКТ система потенцијалним безбедносним слабостима и предузима одговарајуће мере које се односе на уклањање познатих слабости или примену мера заштите.

Анализа дневника активности (*activitylog, history, secutylog, transactionlog* и др.) врши се ради идентификације потенцијалних слабости ИКТ система и предлагања потребних мера за њихово отклањање.

Комора води и податке који су потребни за подршку уорављања техничким рањивостима, а односе се на продавца хардвера и софтвера, серијске бројеве опреме, бројеве верзија инсталираних програма, размештај опреме, аутора софтвера и лица која су задужена за одржавање функционалности инсталираних програма.

1. **Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање систем**

**Члан 48.**

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника.

Уколико није могуће извести ревизију ИКТ система у току радног времена због ометања пословног процеса, иста се врши ван редовног радног времена уз претходно добијену сагласност руководиоца Службе и Председника Коморе и обавља се у присуству запослених у Служби Коморе.

1. **Заштита података у комуникационим мрежама укључујући уређаје и водове**

**Члан 49.**

Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мреже са допуњеним функцијама, решења за управљање безбедношћу информација, као што су заштитне преграде и системи за откривање упада.

Ради заштите података у комуникационим мрежама, уређајима и водовима, врши се њихова контрола, записивање и заштита од неовлашћеног приступа.

У мрежи су међусобно раздвојене групе информационих услуга корисника и информациони систему, а администратор мреже је одговоран за управљање мрежом и благовремено предузимање мера ради отклањања евентуалних неправилности.

Заштита података се врши и постављањем комуникационих каблова и каблова за напајање у зиду или каналицама тако да се онемогући неовлашћени приступ и могуће оштећење комуникационих каблова и каблова за напајање.

1. **Безбедност подата који се преносе унутар Коморе, као и између Коморе и лица ван Коморе**

**Члан 50.**

Заштита података који се преносе комуникационим средствима унутар Коморе, између Коморе и лица ван Коморе обезбеђује се утврђивањем и поштовањем одговарајућих правила, процедура, потписивањем уговора и споразума и применом адекватних контрола.

Употреба електронске поште мора бити у складу са правилима, безбедна и сигурна у складу са позитивним прописима и пословном праксом у тој области.

Електронска поште се може користити искључиво за пословне потребе, а подаци које та комуникација садржи или у њиховом прилогу, морају бити у складу са стандардима заштите података.

Споразуми о поверљивости и неоткривању података обавезују потписнике споразума да их штите, користе и објављују на одговоран и ауторизован начин.

1. **Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система**

**Члан 51.**

Комора је у обавези да обезбеди безбедност информација у току животног циклуда ИКТ система који укључује фазе његовог конципирања, спецификације, пројектовање, развијање, тестирање, примену, коришћење, одржавање и на крају повлачење из употребе.

Питање безбедности се анализира у раним фазама пројектовања информационог система.

О успостављању новог ИКТ система, односно о увођењу нових делова и изменама постојећих делова, води се посебна евиденција. Документација мора да садржи описе свих процедура, а посебно оних које се односе на безбедност ИКТ система.

Приликом постављања захтева за набавку новог информационог система или за побољшање постојећег морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору о куповини информационих добара се дефинишу захтеви безбедности.

Технички надзор врши лице са којим Комора има закључен уговор о одржавању ИКТ система.

1. **Заштита података који се користе за потребе тестирања ИКТ система односно делова система**

**Члан 52.**

Под тестирањем ИКТ система и тестирањем делова система подразумева се низ радњи и поступака који обухватају процене промена стања система, односно делова система који су изложени променама, као и узрока насталих промена.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера уз обезбеђивање копије постојећег система како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

За тестирање и потребе испитивања користе се подаци који нису осетљиви, који се штите, чувају и контролишу на одређени начин. Резултати тестирања се чувају за све време животног века ИКТ система који је тестиран.

1. **Заштита средстава ИКТ система Коморе која су доступна пружаоцима услуга**

**Члан 53.**

Уговори које закључује Комора са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација морају садржати уговорну одредбу о заштити и чувању поверљивих информација, података и документације.

Пружаоци услуга у делу софтверских решења имају право на приступ само оним подацима који се налазе у бази података који су део софтвера који су они израдили и за које је постоји уговор дефинисан приступ.

Администратор мреже има право приступа подацима, у свим софтверским програмима који су у употреби у Комори, без права мењања у циљу обезбеђивања услова за правилно и безбедно функционисање мреже.

Пружаоци услуга су дужни да своје обавезе у погледу безбеднисти информација прошире и на своје подуговораче за додатне услуге и производе који су потребни за извршење уговорне обавезе.

Контролу, приступ и надзор над поштовањем уговорених обавеза од стране пружаоца услуга врши Руководилац Службе који обавештава председника Коморе о реализацији уговора.

1. **Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга**

**Члан 54.**

Контролу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са уговором врши руководилац Службе који о томе обавештава председника Коморе, за све време трајања уговора и у периоду од 5 година по престанку уговора, као року који је прописан уговором.

1. **Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама**

**Члан 55.**

У случају било каквог инцидента који може угрозити безбедност ресурса ИКТ система, сваки корисник је дужан да одмах обавести руководиоца Службе и Председника Коморе и предузме мере ради заштите ресурса ИКТ система и спречавања настанка штете.

Комора води евиденцију о свим инцидентима, пријавам инцидената, мера које су предузете за њихово отклањање, поступака који су спроведени у циљу откривања узрока и евентуалних поступака утврђивања одговорности лица које је изазвало инцидента који могу бити дисциплински, прекршајни или кривични.

На основу прикупљених података, врши се анализа узрока и предузимају мере како би се смањила вероватноћа њиховог понављања и процењује могућност настанка будућих инцидената и смањивање њихових последица.

**Члан 56.**

Уколико је реч о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо – комуникационим системима од посебног значаја, Комора је дужна да обавештење о инциденту достави министарству надлежном за информациону безбедност, министарству унутрашњих послова, сви државним органима са којима се врши размена података и регулаторном телу за електронске комуникације.

1. **Мере које обезбеђују континуитет обављања посла у ванредним околностима**

**Члан 57.**

Комора примењује мере које обезбеђују континуитет у обављању послова и у ванредним околностима самостално и у сарадњи са пружаоцима услуга са којима ума закључене уговоре.

Сви запослени у Служби Коморе су дужни да спроводе прописане процедуте за функционисање ИКТ система у ванредним околностима.

1. **ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ**

**Члан 58.**

У случају настанка промена које могу наступити услед техничко – технолошких, кадровских, организационих промена у ИКТ систему и догађаја а глобалном и националном нивоу који могу нарушити информациону безбедност, извршиће се потребне измене овог Правилника са циљем његовог обезбеђења.

1. **ПРОВЕРА ИКТ СИСТЕМА**

**Члан 59.**

Комора је обавезна да врши проверу ИКТ система најмање једном годишње ради провере адекватности предиђених мера заштите, утврђених процедура, овлашћења и одговорности и евентуалних нарушавања безбедности ИКТ система, разлозима за настанак повреда, последицама и предузетим мерама, о чему се сачињава посебан извештај који се доставља Управном одбору Коморе.

1. **ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ**

**Члан 60.**

Правилник о безбедности информационо – комуникационих система Адвокатске коморе Србије усваја Управни одбор Адвокатске коморе Чачак.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли и интернет страници Коморе.

Дел.број \_\_\_\_\_\_\_\_/20

\_\_\_\_\_\_.\_\_\_\_\_\_.2020.

ПРЕДСЕДНИК

АДВОКАТСКЕ КОМОРЕ ЧАЧАК

Адв.Миодраг Алексић

Правилник о безбедности информационо комуникационих система Адвокатске коморе Чачак објављен је на огласној табли и интернет страници Адвокатске коморе Чачак , дана \_\_\_\_\_.\_\_\_\_\_\_.2020. и ступио је на снагу \_\_\_\_\_.\_\_\_\_\_\_.2020.

ПРЕДСЕДНИК

АДВОКАТСКЕ КОМОРЕ СРБИЈЕ

Адв.Миодраг Алексић